Challenge Type: Forensics

Difficulty: Easy

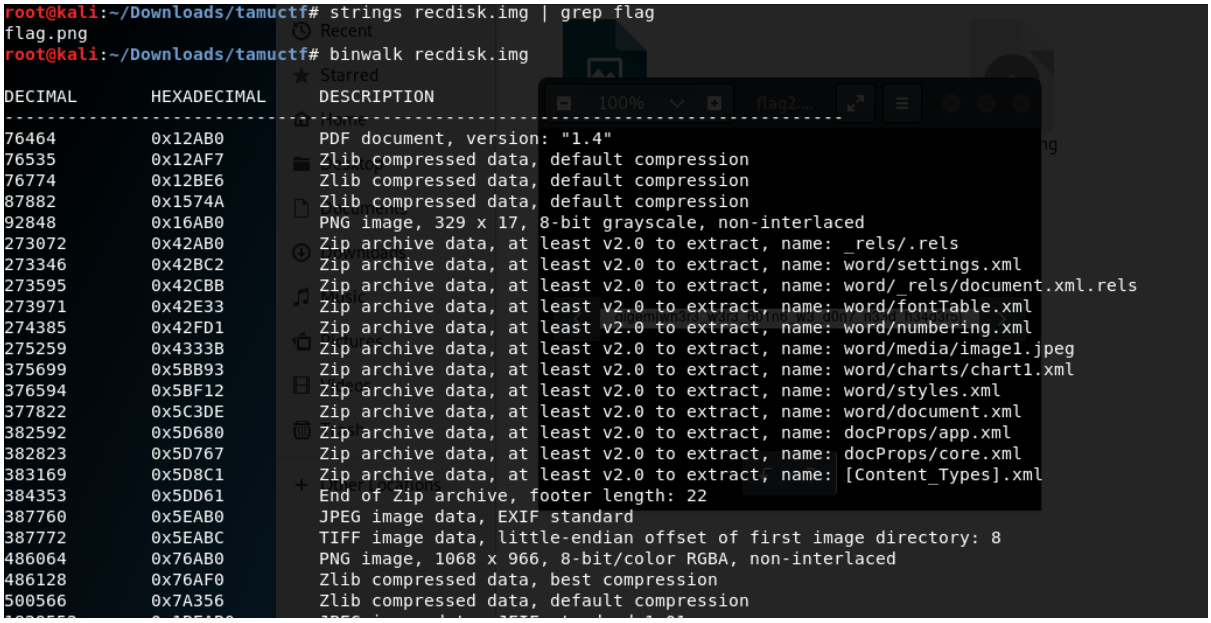
For this challenge, we are given a file called “recdisk.img”. We have to extract the flag from this.

As a part of my preliminary checks for Forensic challenges, I do the below

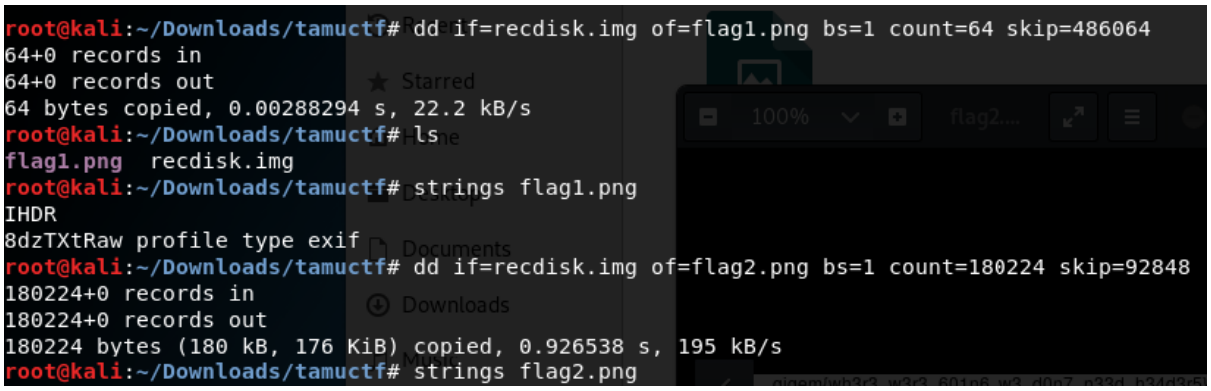
1. Use the ***strings*** command to see if the flag is present as plaintext in the file.
2. Use ***Binwalk*** to check for embedded files.

Applying those on recdisk.img, we get to know that

1. There is a file called *flag.png* in it.
2. There are 2 png images embedded(indices 92848 and 486064).



Now, its very likely that the flag is in one of these 2 png files. So we extract them using the *dd* command and name them *flag1.png* and *flag2.png*.



I first thought of using *strings* again to see if that got me the flag. It did not but I was able to see it after opening *flag2.png*.

Flag: gigem{wh3r3_w3r3_601n6_w3_d0n7_n33d_h34d3r5}